3354:1-20-09 Identity theft policy.

(A) Purpose and leadership.

(1) Identity theft is a serious concern in modern society. The College creates, obtains, and stores personally-identifiable financial and other sensitive information, and desires to ensure appropriate measures are taken to prevent identity theft involving such information. Therefore, the College shall maintain an active identity theft program in accordance with federal trade commission regulations enacted at 16 C.F.R. 681 et. seq. (often referenced as the "red flag rule"). This identity theft policy shall be supported by an "identity theft procedure."

(2) The vice president for administration and finance shall serve as "program administrator," leading development, implementation, and oversight of the identity theft program.

(B) Identifying red flags.

(1) The program should identify red flags for covered accounts and incorporate those red flags into the program.

(a) The program should incorporate the following risk factors in identifying relevant red flags for covered accounts:

(i) The types of covered accounts offered or maintained by the College.

(ii) The methods provided by the College to open covered accounts.

(iii) The methods provided by the College to access covered accounts.

(iv) The College's experience, if any, with identity theft.

(b) The program should incorporate appropriate red flags from relevant experiences and sources, including without limitation:

(i) Incidents of identity theft previously experienced.

(ii) Methods of identity theft that reflect changes in risk.

(iii) Regulatory or professional guidance.

(c) As appropriate, the program shall include relevant red flags from the following categories of risk factors:

(i) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services.

(ii) The presentation of suspicious documents.

(iii) The presentation of suspicious personal identifying information.

(iv) The unusual use of, or other suspicious activity related to, a covered account.

(v) Notice from customers, employees, students, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

(C) Detecting and responding to red flags.

The College's identity theft procedure should address the detection of red flags in connection with the opening of new covered accounts and existing covered accounts. The identity theft procedure should provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The responses should be commensurate with the degree of risk posed.

(D) Updating the identity theft program.

The College should periodically, and at least annually, update the identity theft program (including the identity theft policy and procedure), in accordance with appropriate factors, which may include:

(1) The experiences of the organization with identity theft.

(2) Changes in methods of identity theft.

(3) Changes in methods to detect, prevent and mitigate identity theft.

(4) Changes in the types of accounts that the organization offers or maintains.

(5) Changes in the business arrangements of the organization, including without limitation, alliances, joint ventures, and service provider arrangements.

(E) Definitions.

(1) “Covered accounts” are the College’s deferred payment plans, emergency loans, perkins loans, and my tri-c card accounts.

(2) “Identifying information” is “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including without limitation: name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, student identification number, employee identification number, computer’s internet protocol address, and routing code.

(3) “Identity theft” is a “fraud committed or attempted using the identifying information of another person without authority.”

(4) “Red flag” means a “pattern, practice, or specific activity that indicates the possible existence of identity theft.”

(F) Methods for administering the program.

In administering the identity theft program, the program administrator shall be responsible for:

(1) Training of College staff on the program.

(2) Requiring and reviewing reports on compliance with this program. The identity theft procedure should include appropriate details about this reporting process.

(3) Leading prevention and mitigation efforts in particular circumstances.

(4) Monitoring and ensuring College compliance with the identity theft policy and procedure.

(5) Overseeing the activities of service providers performing activities related to covered accounts to ensure that such activities are conducted pursuant to reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

(G) The president or the president's designee is hereby directed to take all steps necessary and appropriate for the effective implementation of this policy.

Effective date: December 3, 2009